Wat is relay attack

In de pers worden verschillende diefstalmethodes aangehaald, waarbij dieven gebruik maken van nieuwe technieken zoals het zogenaamde “Relay Attack”. Doelwit zijn voertuigen die zijn voorzien van “**keyless entry**” en “**keyless start of go**”. Het signaal van de zogenaamde “smart key” wordt illegaal afgelezen en verlengd. Waar normaal de afstand tussen voertuig en handzender max. één meter moet zijn om hem te kunnen openen, kan dit nu op een afstand van enkele honderden meters door het signaal te kopiëren en te “verlengen”.

Hoe werkt het in de praktijk?

Een auto staat in een straat en de sleutels liggen achter een gesloten voordeur. De eigenaar heeft zijn auto normaal afgesloten. Als de auto is voorzien van de comfort optie keyless entry, dan kunnen criminelen hier echter misbruik van maken. Dat gaat als volgt: één persoon vangt het signaal van de handzender op die achter de voordeur ligt, terwijl een tweede persoon, die bij de auto staat, met het verlengde signaal de auto opent, start en meeneemt. Voor het opvangen en verlengen van het signaal is wel speciale apparatuur noodzakelijk.

Wat kunt u er tegen doen?

Met een VbV – SCM goedgekeurde startonderbreker met een “eigen autorisatie”, is deze manier van diefstal onmogelijk. De startonderbreker werkt onafhankelijk van de keyless functies van de auto. Zo kan de dief misschien nog wel de auto ontgrendelen, maar niet starten en wegrijden.

Henk van Vliet
Certificatie manager Kiwa- SCM

Kiwa SCM is de Certificatie Instelling die zich bezighoudt met voertuigbeveiliging. Zij kennen de verschillende diefstalmethodes en controleren of voertuigen hier tegen bestand zijn. Kiwa- SCM werkt daarbij samen met Stichting VbV, de politie, Stichting AVc, en diefstalonderzoeksbureaus. Met Kiwa SCM gecertificeerde beveiliging heb je minder kans dat je auto gestolen wordt.

Fabrikant- Verzekering- of consumentprobleem?

Stel nu dat u uw auto om 7 uur heeft geparkeerd en om 8 uur ziet dat uw auto is gestolen. U geeft aan uw verzekeraar door wat er is gebeurd en op welke tijdstippen. De verzekeraar heeft de mogelijkheid om de sleutel uit te laten lezen en stelt vast dat de auto is gestart met uw eigen sleutel om bijvoorbeeld half 8. U heeft dan toch iets uit te leggen aan de verzekeraar.
Een dergelijke casus over relay attack is ook onderwerp van gesprek geweest tijdens een onlangs gehouden meeting van AVc met Europese koepels van autoconsumenten (FIA), verzekeraars (Insurance Europe / IE) en autofabrikanten (ACEA).
Een paar quotes hierover:

IE: ‘… sommige verzekeraars laten hun klanten de keyless optie uitschakelen.’

FIA: ‘… dat is raar; de consument koopt een dure auto, betaalt goed geld voor zo’n optie en die zou hij vervolgens moeten uitschakelen?’

IE: ‘… andere verzekeraars vereisen een extra beveiliging; als die er niet op zit kan de verzekeraar niet vaststellen of de auto via relay attack gestolen is of dat de eigenaar in het complot zit.’

AVc: '… wij hebben nog niet gehoord van problemen over de vergoeding van diefstalschade. Onsteelbare auto's bestaan niet; daarom bestaat er zoiets als een diefstalrisicoverzekering.
FIA: '… wij vinden het onjuist dat de klant voor een falend systeem moet opdraaien. Uiteindelijk zijn consumenten de dupe van diefstallen. Wij verwachten van fabrikanten dat ze auto's leveren die veilig zijn, ook tegen hackers. Relay attack is al meer dan een jaar bekend, fabrikanten blijven de systemen gewoon verkopen; ze zouden die echt eerst hacker-proof moeten maken.'
ACEA: …'onze klanten vragen om keyless entry, dus dat leveren we.'

Dit geheel overziend is de tijd rijp dat consumenten weten wat ze kopen, zodat ze niet verrast zijn als ze voor een dubbele investering staan: eerst betalen voor een 'comfort' optie en dan nog eens voor extra beveiliging.